OFFICE OF THE INSPECTOR GENERAL

SOCIAL SECURITY ADMINISTRATION

THE SOCIAL SECURITY ADMINISTRATION'S COMPLIANCE WITH THE *FEDERAL INFORMATION SECURITY MANAGEMENT ACT OF 2002* FOR FISCAL YEAR 2012

November 2012 **A-14-12-12120**

AUDIT REPORT

Mission

By conducting independent and objective audits, evaluations and investigations, we inspire public confidence in the integrity and security of SSA's programs and operations and protect them against fraud, waste and abuse. We provide timely, useful and reliable information and advice to Administration officials, Congress and the public.

Authority

The Inspector General Act created independent audit and investigative units, called the Office of Inspector General (OIG). The mission of the OIG, as spelled out in the Act, is to:

- **Conduct and supervise independent and objective audits and investigations relating to agency programs and operations.**
- **Promote economy, effectiveness, and efficiency within the agency.**
- **Prevent and detect fraud, waste, and abuse in agency programs and operations.**
- **Review and make recommendations regarding existing and proposed legislation and regulations relating to agency programs and operations.**
- **Keep the agency head and the Congress fully and currently informed of problems in agency programs and operations.**

To ensure objectivity, the IG Act empowers the IG with:

- **Independence to determine what reviews to perform.**
- **Access to all information necessary for the reviews.**
- **Authority to publish findings and recommendations based on the reviews.**

Vision

We strive for continual improvement in SSA's programs, operations and management by proactively seeking new ways to prevent and deter fraud, waste and abuse. We commit to integrity and excellence by supporting an environment that provides a valuable public service while encouraging employee development and retention and fostering diversity and innovation.

OIG Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

MEMORANDUM

Date: November 15, 2012 Refer To:

To: The Commissioner

From: Inspector General

Subject: The Social Security Administration's Compliance with the *Federal Information Security Management Act of 2002* for Fiscal Year 2012 (A-14-12-12120)

OBJECTIVE

Our objective was to determine whether the Social Security Administration's (SSA) overall information security program and practices were effective and consistent with the requirements of the *Federal Information Security Management Act of 2002* (FISMA) as defined by the Department of Homeland Security (DHS).

BACKGROUND

FISMA provides the framework for securing the Government's information and information systems. All agencies must implement the FISMA requirements and report annually to the Office of Management and Budget (OMB), DHS, and Congress on the adequacy and effectiveness of their security programs. FISMA requires that each agency develop, document, and implement an agency-wide information security program.[1] Each agency head is responsible for providing information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of agency information and information systems.[2]

FISMA also requires that each agency's Inspector General (IG), or an independent external auditor, perform an independent evaluation of the agency's information security program and practices to determine their effectiveness.[3] Each evaluation shall

- test the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems and

[1] Pub. L. No. 107-347, Title III, Section 301 § 3544(b); 44 U.S.C. § 3544(b).

[2] Pub. L. No. 107-347, Title III, Section 301 § 3544(a)(1)(A); 44 U.S.C. § 3544(a)(1)(A).

[3] Pub. L. No. 107-347, Title III, Section 301 §§ 3545(a)(1) and (b)(1); 44 U.S.C. §§ 3545(a)(1) and (b)(1).

- assess compliance with FISMA requirements, and related information security policies, procedures, standards, and guidelines.[4]

DHS is responsible for overseeing compliance with FISMA and developing analyses to assist in OMB's annual report to Congress on Federal agencies' compliance with FISMA.[5] To fulfill its responsibilities, DHS provided annual FISMA reporting instructions for Federal agencies, including IGs. Specifically for IGs, DHS defined 11 FISMA security program components. For each component, IGs must respond to the following areas.

1. Has the Agency established an enterprise-wide program consistent with FISMA requirements, OMB policy, and applicable National Institute of Standards and Technology (NIST) guidance? If yes, besides the improvement opportunities that may have been identified by the IG, does the program include the attributes identified by DHS?

2. Provide any additional information on the effectiveness of the program.

SCOPE AND METHODOLOGY

We contracted with Grant Thornton, LLP, (GT) to audit SSA's Fiscal Year (FY) 2012 financial statements.[6] Because of the extensive internal control system review completed as part of that work, some of our FISMA requirements were incorporated into GT's financial statement audit information technology (IT)-related work. This evaluation included the *Federal Information System Controls Audit Manual* level reviews of SSA's financial-related information systems. GT also performed an "agreed-upon procedures" engagement using FISMA, OMB, DHS, NIST guidance, the *Federal Information System Controls Audit Manual*, and other relevant security laws and regulations. We evaluated GT's work and performed additional FISMA testing for this review.

To assess whether SSA met FISMA requirements as defined by DHS, we used DHS guidance[7] to test the compliance and effectiveness of agencies' security policies, procedures and practices. For the 11 FISMA security program component metrics and our responses to those metrics, see Appendix B, *Office of the Inspector General Response to FY 2012 Inspector General Federal Information Security Management Act Reporting Metrics*.

---

[4] Pub. L. No. 107-347, Title III, Section 301 §§ 3545(a)(2)(A) and (B); 44 U.S.C. §§ 3545(a)(2)(A) and (B).

[5] OMB, M-10-28, *Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security (DHS)*, July 6, 2010, page 2.

[6] Office of the Inspector General Contract Number GS-23F-8196H, December 3, 2009. The FY 2012 option was exercised in December 2011.

[7] DHS, *FY 2012 Inspector General Federal Information Security Management Act Reporting Metrics*, March 6, 2012.

This report informs Congress and the public about SSA's security performance and fulfills the OMB and DHS requirements under FISMA to submit an annual report to Congress. It provides an assessment of SSA's information security strengths and weaknesses. See Appendix C for more details on our scope and methodology.

RESULTS OF REVIEW

For FY 2012, we determined that SSA had established an overall information security program and practices that were generally consistent with FISMA requirements.[8] However, weaknesses in some of the program's components limited the overall program's effectiveness to adequately protect the Agency's information and information systems. Specifically, GT identified a material weakness over internal controls in its *Independent Auditor's Report.* We also identified additional weaknesses. Based on our evaluation of GT's work and our work, we believe these weaknesses constituted a significant deficiency under FISMA.

FINANCIAL STATEMENT AUDIT MATERIAL WEAKNESS

In FY 2012, GT identified deficiencies in information security controls that, when combined, it considered a material weakness. **A material weakness for financial statement purposes** is a deficiency, or combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected timely.[9] As a result, for FY 2012, GT reported a material weakness in SSA's internal control over its financial statements.

GT stated that SSA had attempted to strengthen controls over its systems and address the outstanding significant deficiency in information security. However, GT's FY 2012 testing identified the following security weaknesses that, when aggregated, met the definition of a material weakness for financial statement purposes.

- Lack of monitoring and policy implementation related to the configuration and information content of SSA's Intranet Webpages. The misconfiguration of some of SSA systems allowed GT to obtain security information and personally identifiable

[8] Our conclusion was based on our assessment of SSA's compliance with DHS' *FY 2012 Inspector General Federal Information Security Management Act Reporting Metrics*, March 6, 2012. As indicated in Appendix B, we determined that SSA established all 11 security program components, which were generally consistent with Federal guidance. The 11 components established by SSA included the vast majority of attributes identified by DHS. However, we also noted improvement opportunities for many attributes.

[9] The definition of a material weakness for financial statement internal control is provided by the Statement on Auditing Standards Number 115, *Communicating Internal Control-Related Matters Identified in an Audit*.

information (PII)[10] from SSA's Intranet. This issue increases the risk that SSA's sensitive information could be used inappropriately.

- Lack of controls related to the identification and monitoring of high-risk programs operating on the Agency's mainframe.[11] SSA did not conduct impact assessments to determine whether significant changes to its mainframe programs created any security implications. In addition, SSA management did not have a comprehensive process to periodically review privileged programs added to SSA's mainframe environment. Privileged programs are considered high-risk because they could bypass mainframe system security.

- Insufficient vulnerability testing conducted by the Agency to identify critical weaknesses in its IT environment. For the second year in a row, GT was able to gain access to restricted information and take control of SSA's Windows network during internal penetration testing.[12] GT reported that management's failure to conduct robust enterprise-focused penetration testing increases the risk that unauthorized access may occur and go undetected, allowing privileged information or critical infrastructure to be compromised.

- Lack of a comprehensive profile and access recertification program. GT found that SSA developed identity and access management policies and procedures to periodically reassess the content of security access profiles.[13] However, the Agency had not consistently implemented these policies and procedures. Further, GT's testing identified personnel with inappropriate access.

- Lack of appropriate controls to prevent unauthorized access to the Agency's production environment. Agency management stated that a control was in place to allow programmers highly monitored and time-limited access to production data. However, GT identified software programmers with access to SSA's production data that bypassed this control. SSA management indicated this issue resulted from

---

[10] OMB, M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, July 2006, page 1, defines PII as any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information that can be used to distinguish or trace an individual's identity, such as their name, Social Security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information that is linked or linkable to an individual.

[11] International Business Machines Corp. defines a mainframe as computers that can support thousands of applications and input/output devices to simultaneously serve thousands of users. A mainframe is the central data repository, or hub, in a corporation's data processing center, linked to users through less powerful devices such as workstations or terminals.

[12] GT used a different method to take control of SSA's Windows network this year.

[13] A profile is one of SSA's primary access control mechanisms. Each profile contains a unique mix of facilities and transactions that determines what access to systems resources a specific position needs.

human error, and that no current control would have identified this error in a timely manner. In addition, GT identified instances where this control was used, but access was not timely approved and reviewed. Despite these weaknesses, GT did not find any unauthorized changes to the Agency's data.

WEAKNESSES IN SOME COMPENSATING CONTROLS

GT discussed the security weaknesses it identified with SSA management and staff. Agency management stated that compensating controls existed to mitigate the risks created by the security weaknesses. However, GT's FY 2012 financial statement audit testing and our audits identified weaknesses in some of the compensating controls identified by SSA. This included control deficiencies in the Agency's change control process and physical and logical access controls. For example, GT noted weaknesses over the approval and documentation for changes to SSA software applications. Further, we found that a contractor employee maintained physical access to SSA facilities for approximately 1 year after the contractor employee was deemed unsuitable for employment.[14] In addition, we found that a disability determination services' employee's system user identification was used after the employee was terminated.[15]

ADDITIONAL SECURITY WEAKNESSES

In addition to the security weaknesses identified above, our FY 2012 FISMA testing identified some security weaknesses related to key components of SSA's information security program. These key components include Continuous Monitoring, Configuration Management, Identity and Access Management, Risk Management, and Contractor Systems Oversight. In prior years, we have also identified weaknesses in these areas. We highlight some key weaknesses below.

- Continuous Monitoring:[16] The Agency had not fully implemented its continuous monitoring strategy. For example, SSA had not implemented compliance monitoring tools for all of its platforms.[17] Further, SSA needed to assess and validate the technical capacity of each continuous monitoring tool to meet NIST requirements. Finally, SSA's continuous monitoring activities did not provide the near real-time information required for Agency officials to proactively manage the Agency's information security program in accordance with OMB and NIST requirements.

[14] The contractor employee was immediately removed from the contract after the appropriate SSA personnel were notified.

[15] Management confirmed that no transactions were executed with the terminated employee's user identification after termination.

[16] Continuous Monitoring maintains ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

[17] A platform is a hardware and/or software architecture that serves as a foundation or base. An operating system, like Windows, is an example of a platform.

- Configuration Management:[18] SSA used risk models for its platforms to prescribe security settings and manage risk. However, SSA had not documented risk models for all of its platforms. Further, the Agency did not perform vulnerability scans of all platforms to determine whether prescribed security settings were implemented. Moreover, the vulnerability scans and penetration testing performed by GT identified a number of security weaknesses.

- Identity and Access Management:[19] SSA scanned its network to identify connected hardware, but as of the date of this review, it had been unable to categorize all types of hardware and their associated operating systems.

- Risk Management:[20] SSA had weaknesses in its security governance structure. The Agency's central technical security component did not have control over regional office Intranet Websites. In addition, SSA lacked a centralized process to authorize hardware devices before they were connected to the Agency's network.

- Contractor Systems Oversight:[21] SSA did not maintain a complete inventory of all contractor systems and services and did not ensure all contractor systems and services met Federal security requirements. Specifically, we identified seven systems and services that met the FISMA criteria for contractor systems but either

[18] From a security point of view, Configuration Management provides assurance that the system in operation is the correct version (configuration) of the system and that any changes to be made are reviewed for security implications.

[19] Identity and Access Management includes policies to control user access to information system objects, including devices, programs, and files. The identification of devices with Internet Protocol addresses attached to an agency's network is included under the Identity and Access Management section of DHS' *FY 2012 Inspector General Federal Information Security Management Act Reporting Metrics*, March 6, 2012.

[20] "Risk Management is the process of managing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system." NIST Special Publication 800-53, Rev. 3, page B-11.

[21] Agencies are responsible for ensuring that appropriate security controls are in place over contractor systems used or operated by contractors or other entities (such as other Federal or state agencies) on behalf of an agency. We used OMB M-12-20, *FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, Frequently Asked Questions, September 27, 2012, pages 15 to 16, to determine the purview of the Agency's FISMA responsibilities for contractor systems. SSA disagreed with our interpretation. However, this OMB guidance explicitly provides that "Because FISMA applies to both information and information systems used by the agency, contractors, and other organizations and sources, it has somewhat broader applicability than prior security law. That is, agency information security programs apply to all organizations (sources) which process, store, or transmit Federal information- or which operate, use, or have access to Federal information systems (whether automated or manual) -on behalf of a Federal agency." OMB, M-12-20 at page 16.

were not included in the Agency's systems inventory or were not identified as a contractor system or service, as required by FISMA guidance. Further, some of SSA's contracts did not include Federal security requirements, as required by FISMA guidance.

FISMA SIGNIFICANT DEFICIENCY

OMB defines a FISMA significant deficiency as ". . . a weakness in an agency's overall information systems security program or management control structure, or within one or more information systems, that significantly restricts the capability of the agency to carry out its mission or **compromises the security of its information, information systems, personnel, or other resources, operations, or assets.** In this context, the risk is great enough that the agency head and outside agencies must be notified and immediate or near-immediate corrective action must be taken."[22]

SSA administers two of the nation's largest entitlement programs, the Old-Age, Survivors, and Disability insurance program and the Supplemental Security Income program. These programs touch the lives of virtually every American. It is imperative that SSA protect these programs by ensuring the safety and security of its information systems and the data contained in them.

Based on our evaluation of the work performed by GT and the results of our additional FISMA work, we concluded that the risk and severity of SSA's information security weaknesses were great enough to constitute a significant deficiency under FISMA. These weaknesses could result in losses of confidentiality, integrity, and availability of SSA information systems and data.[23] Given the complex systems and magnitude of sensitive information housed on SSA's systems, any loss of confidentiality, integrity, or availability of Agency systems or data could have a significant impact on the public and the nation's economy. For example, during its internal penetration testing, GT was able to take control of SSA's Windows network and obtain many records containing PII. In addition, GT noted concerns related to the identification and monitoring of high risk programs operating on the mainframe. Without performing specific assessments of the impact of program changes to the system security framework, there is an increased risk that the security posture and controls may be bypassed or compromised. Finally, GT identified programmers with access to production data that bypassed SSA's process to monitor and limit such access. Specifically, GT identified programmers with

---

[22] OMB, M-12-20, *FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, Frequently Asked Questions, September 27, 2012, page 26.

[23] **Confidentiality** means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information. **Integrity** means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity. **Availability** means ensuring timely and reliable access to and use of information. Pub. L. No. 107-347, Title III, Section 301 § 3542(b)(1)(A) to (C), 44 U.S.C. § 3542(b)(1)(A) to (C).

unmonitored access to production data for a benefit application. This issue increases the risk that programmers could make unauthorized changes to the production environment without detection.

The security deficiencies identified above, when aggregated, created a weakness in SSA's overall information systems security program that, in our opinion, significantly compromised the security of its information and information systems. We also believe that the risk was great enough that the agency head and outside agencies must be notified and immediate or near-immediate corrective action must be taken.[24]

UNDERLYING CAUSES FOR SSA's FINANCIAL STATEMENT AUDIT MATERIAL WEAKNESS AND FISMA SIGNIFICANT DEFICIENCY

Based on our testing and evaluation of GT's work, we believe the following items caused the Agency's material weakness and FISMA significant deficiency.

1. SSA had not fully implemented a comprehensive and robust continuous monitoring program based on a sound configuration management program. Without a robust continuous monitoring program that includes integrated and operating continuous monitoring tools and the capacity to report SSA's security state to appropriate Agency officials, the Agency had a limited ability to make timely risk management decisions.
2. SSA had a decentralized governance structure for IT security. This resulted in a system misconfiguration that enabled GT, without detection, to obtain PII and take control of SSA's Windows network.
3. SSA needed to strategically allocate sufficient resources to resolve or prevent high-risk security weaknesses more timely. This includes the use of more effective security testing methods, such as broad penetration testing techniques.

AGENCY EFFORTS TO RESOLVE SECURITY WEAKNESSES

It should be noted that SSA took action to address some of its security weaknesses identified by GT and us:

Lack of monitoring and policy implementation related to the configuration and information content of SSA's Intranet Webpages. SSA stated it was conducting a Web vulnerability assessment. In addition, the Agency stated it had purchased and was deploying a data loss protection tool.

[24] Significant deficiencies identified under FISMA must be reported as material weaknesses in the annual *Federal Managers' Financial Integrity Act of 1982* report. OMB Circular A-123 Revised, *Management's Responsibility for Internal Control*, Section IV B, December 21, 2004.

Lack of controls related to the identification and monitoring of high-risk programs operating on the Agency's mainframe. The Agency removed one high-risk privileged program identified by GT. Furthermore, SSA stated it was expanding its review process to include all mainframe privileged programs.

Insufficient vulnerability testing conducted by the Agency to identify critical weaknesses in its IT environment. SSA documentation indicated that over the past 10 years, the Agency has performed some penetration testing. Between 2009 and 2011, SSA used some of the funding traditionally used for penetration testing for other information security purposes. However, SSA stated that in 2012, it began performing penetration testing with an open and dynamic scope. The Agency hired three contractor employees in September 2012 to perform targeted internal penetration testing to identify security weaknesses of SSA's networks.

Lack of a comprehensive profile and access recertification program. In FY 2011, SSA issued two policies governing security profiles.[25] In addition, the Agency assembled a workgroup to address its access control weaknesses. The workgroup tested a commercial tool to manage the profile review process for SSA employee and contractor access. The Agency began using the tool in FY 2012. SSA planned to remediate some access control issues by fully implementing its profile and access recertification program in early FY 2013.

Lack of appropriate controls to prevent unauthorized access to the Agency's production environment. SSA management stated that the Agency removed the access of the programmers identified in GT's testing. Moreover, the Agency stated its triennial access recertification will identify these issues in the future, and SSA was exploring options to alert the Agency if programmers gain access to the production environment.

Continuous monitoring strategy not fully implemented. SSA developed a continuous monitoring strategy, but the strategy had not been fully implemented. SSA discussed its preliminary plan to implement its continuous monitoring strategy with us. To build upon its continuous monitoring strategy, SSA has been evaluating the ability of its continuous monitoring tools to ensure compliance with Federal requirements and Agency policies and procedures. Further, SSA management stated that after the continuous monitoring tool evaluations are completed, it will have a better idea of the timeframe needed to fully implement its continuous monitoring strategy. The Agency plans to complete the continuous monitoring tool evaluations by the end of calendar year 2012. Finally, SSA is evaluating which security deficiencies identified by GT could be resolved by fully implementing its continuous monitoring strategy.

---

[25] SSA, *Security Profile Administration Processes Final Mainframe Administration Standards*, May 10, 2011, and SSA, *Security Profile Administration Processes Profile Naming Conventions*, October 28, 2010.

CONCLUSION AND RECOMMENDATIONS

For FY 2012, we determined that SSA's overall information security program and practices were generally consistent with FISMA requirements. However, weaknesses in some components of the program limited the overall program's effectiveness to adequately protect the Agency's information and information systems. We noted that GT reported a material weakness over SSA's internal controls for the Agency's financial statement audit. After considering this material weakness, its underlying causes, and the results of our FISMA-related work, we concluded that the risk and severity of SSA's information security weaknesses were great enough to constitute a significant deficiency under FISMA.

SSA needed to effectively protect its mission-critical assets. Without appropriate security, the Agency's systems and the sensitive data they contain are at risk. Some weaknesses identified in this report could cause the Agency's systems and data to lose confidentiality, integrity, and availability to some degree. Given the complex systems and magnitude of sensitive information housed on SSA's systems, any loss of the confidentiality, integrity, or availability of Agency systems or data could have a significant impact on the public.

To improve the effectiveness of SSA's overall information security program and to address the material weakness, GT recommended that SSA management consider implementing:

- Monitoring controls designed to identify configurations in the SSA network and systems environment that do not comply with the SSA system configuration policy. In addition, management should consider implementing controls to identify and track content on SSA's Intranet Webpages that may pose a risk to the security of SSA systems or the confidentiality of SSA data.
- A comprehensive program to identify and monitor high-risk programs operating on the mainframe. Consider including the identification of programs that may pose security risks to the SSA mainframe before they are loaded onto the production environment.
- Comprehensive enterprise-wide security vulnerability testing, including simulated penetration attacks, to identify critical weaknesses in the IT environment that may not be identified by the current control processes.
- A comprehensive profile and access recertification program.
- Additional controls to prevent unauthorized programmer access to the production environment.

We reiterate GT's recommendations and believe these recommendations address the financial statement audit material weakness and FISMA significant deficiency. In addition, our prior FISMA reports identified issues related to SSA's (1) continuous monitoring, (2) configuration management, (3) identity and access management, (4) risk

management, and (5) contractor systems oversight. We affirm our prior recommendations in these areas and encourage the Agency to continue implementing them.

Patrick P. O'Carroll, Jr.

Appendices

APPENDIX A – Acronyms

APPENDIX B – Office of the Inspector General Response to *FY 2012 Inspector General Federal Information Security Management Act Reporting Metrics*

APPENDIX C – Scope and Methodology

APPENDIX D – The Social Security Administration's Major Systems

APPENDIX E – OIG Contacts and Staff Acknowledgments

Acronyms

DHS	Department of Homeland Security
FISMA	*Federal Information Security Management Act of 2002*
FY	Fiscal Year
GT	Grant Thornton LLP
IG	Inspector General
IT	Information Technology
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PII	Personally Identifiable Information
Pub. L. No.	Public Law Number
SSA	Social Security Administration
U.S.C.	United States Code

Office of the Inspector General Response to *FY 2012 Inspector General Federal Information Security Management Act Reporting Metrics*[1]

Section 1: CONTINUOUS MONITORING MANAGEMENT

1.1. Has the Organization established an enterprise-wide continuous monitoring program that assesses the security state of information systems that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines?

Yes

If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

1.1.1. Documented policies and procedures for continuous monitoring.

Yes

1.1.2. Documented strategy and plans for continuous monitoring.

Yes

1.1.3. Ongoing assessments of security controls (system-specific, hybrid, and common) that have been performed based on the approved continuous monitoring plans.

Yes

Comments: To date, SSA had not fully implemented its continuous monitoring program. For example, the Agency had not developed risk models for some of the hardware and software connected to its network. Therefore, the Agency did not continually monitor these operating system platforms and applications.

1.1.4. Provides authorizing officials and other key system officials with security status reports covering updates to security plans and security assessment reports, as well as POA&M additions and updates with the frequency defined in the strategy and/or plans.

[1] Department of Homeland Security (DHS), *FY 2012 Inspector General Federal Information Security Management Act Reporting Metrics*, March 6, 2012. We extracted the DHS metrics as they were written in the document without editing, except for the citations to Federal guidance at the end of some metrics that we omitted for consistency.

Yes

Comments: SSA's current continuous monitoring could not provide a comprehensive view and near real-time information of the enterprise.

1.2. Please provide any additional information on the effectiveness of the Organization's Continuous Monitoring Management Program that was not noted in the questions above.

Comments: SSA did have a continuous monitoring strategy, but it had not been fully implemented. For example, SSA had identified, evaluated, and implemented, some continuous monitoring tools for its operating environment. However, the Agency needed additional time to ensure the continuous monitoring tools were fully operable within its information system environment. Consequently, SSA's continuous monitoring program could not provide a comprehensive view and near real-time information of the enterprise.

Weaknesses identified in this area contributed to a financial statement audit material weakness identified by Grant Thornton, LLP (GT). Based on our work and evaluation of GT's work, we concluded that SSA had a FISMA significant deficiency.

Section 2: CONFIGURATION MANAGEMENT

2.1. Has the Organization established a security configuration management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines?

Yes

If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

2.1.1. Documented policies and procedures for configuration management.

Yes

2.1.2. Standard baseline configurations defined.

Yes

Comments: The Agency had established baseline configurations for many, but not all, computer platforms.

2.1.3. Assessing for compliance with baseline configurations.

Yes

Comments: We identified security weaknesses in the configuration settings of some SSA computer platforms. Internal penetration

testers were able to obtain security information and personally identifiable information because some of SSA's systems were misconfigured. SSA had taken corrective action to address these issues.

2.1.4. Process for timely, as specified in Organization policy or standards, remediation of scan result deviations.

Yes

2.1.5. For Windows-based components, FDCC/USGCB secure configuration settings fully implemented and any deviations from FDCC/USGCB baseline settings fully documented.

Yes

2.1.6. Documented proposed or actual changes to hardware and software configurations.

Yes

Comments: SSA monitored the hardware devices connected to its network to determine whether they complied with approved risk models and configuration settings. However, the Agency did not conduct impact assessments to determine the security implications for system changes. In addition, management did not have a formally documented process to periodically review the privileged programs added to the Agency's mainframe environment to ensure that all privileged programs are approved, cannot be improperly modified, and are safe. We also identified discrepancies in the approval and documentation of changes to SSA applications.

2.1.7. Process for timely and secure installation of software patches.

Yes

2.1.8. Software assessing (scanning) capabilities are fully implemented.

No

Comments: The Agency had implemented scanning procedures for some, but not all, platforms. SSA did not have a formal process in place for managing or obtaining a comprehensive list of approved software for all devices. However, the Agency had made efforts to develop this process.

2.1.9. Configuration-related vulnerabilities, including scan findings, have been remediated in a timely manner, as specified in Organization policy or standards.

Yes

Comments: Annual vulnerability scans and penetration testing have consistently identified security weaknesses. However, some security weaknesses were fully or partially remediated during the

audit period. Since the Agency does not have risk models for all computer platforms, some configuration-related vulnerabilities went unidentified.

2.1.10. Patch management process is fully developed, as specified in Organization policy or standards.

Yes

2.2. Please provide any additional information on the effectiveness of the Organization's Configuration Management Program that was not noted in the questions above.

Comments: Weaknesses identified in this area contributed to a financial statement audit material weakness identified by GT. Based on our work and evaluation of GT's work, we concluded that SSA had a FISMA significant deficiency.

Section 3: IDENTITY AND ACCESS MANAGEMENT

3.1. Has the Organization established an identity and access management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and identifies users and network devices?

Yes

If yes, besides the improvement opportunities that have been identified by the OIG, does the program include the following attributes:

3.1.1. Documented policies and procedures for account and identity management.

Yes

3.1.2. Identifies all users, including federal employees, contractors, and others who access Organization systems.

Yes

3.1.3. Identifies when special access requirements (e.g., multi-factor authentication) are necessary.

Yes

Comments: We identified programmers with access to production data that bypassed SSA's process to monitor and limit such access.

3.1.4. If multi-factor authentication is in use, it is linked to the Organization's PIV program where appropriate.

Yes

3.1.5. Organization has adequately planned for implementation of PIV for logical access in accordance with government policies.

Yes

3.1.6. Ensures that the users are granted access based on needs and separation of duties principles.

Yes

Comments: Although SSA had an extensive access control program, internal penetration testers were able to take control of SSA's Windows network. Testing also identified personnel with inappropriate access and programmers with access to production data that bypassed SSA's process to monitor and limit such access. The Agency had not consistently implemented policies and procedures to periodically reassess the content of security access profiles. SSA was working to improve its profile and access recertification program and planned for a full implementation in Fiscal Year (FY) 2013.

3.1.7. Identifies devices with IP addresses that are attached to the network and distinguishes these devices from users. (For example: IP phones, faxes, printers are examples of devices attached to the network that are distinguishable from desktops, laptops or servers that have user accounts)

Yes

Comments: Although SSA scanned its network to identify hardware devices connected to it, the Agency had been unable to categorize all hardware devices and their associated operating systems connected to its network. Further, SSA did not have an automated capability to determine whether hardware devices connected to its network were authorized.

3.1.8. Identifies all User and Non-User Accounts (refers to user accounts that are on a system. Examples of non-user accounts are accounts such as an IP that is set up for printing. Data user accounts are created to pull generic information from a database or a guest/anonymous account for generic login purposes that are not associated with a single user or a specific group of users)

Yes

3.1.9. Ensures that accounts are terminated or deactivated once access is no longer required.

Yes

Comments: Although SSA had policies and procedures to terminate access when it is no longer needed, we identified instances where physical and logical access was not removed timely.

3.1.10. Identifies and controls use of shared accounts.

Yes

3.2. Please provide any additional information on the effectiveness of the Organization's Identity and Access Management Program that was not noted in the questions above.

Comments: Weaknesses identified in this area contributed to a financial statement audit material weakness identified by GT. Based on our work and evaluation of GT's work, we concluded that SSA had a FISMA significant deficiency.

Section 4: INCIDENT RESPONSE AND REPORTING

4.1. Has the Organization established an incident response and reporting program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines?

Yes

If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

4.1.1. Documented policies and procedures for detecting, responding to and reporting incidents.

Yes

4.1.2. Comprehensive analysis, validation and documentation of incidents.

Yes

4.1.3. When applicable, reports to US-CERT within established timeframes.

Yes

4.1.4. When applicable, reports to law enforcement within established timeframes.

Yes

Comments: SSA reported incidents to OIG in a timely manner. The Agency did not have an established timeframe for reporting incidents to external law enforcement or the Federal Protective Services. SSA identified incidents reported to external law enforcement or the Federal Protective Services; however, the Agency did not provide police reports for sampled incidents.

4.1.5. Responds to and resolves incidents in a timely manner, as specified in Organization policy or standards, to minimize further damage.

Yes

4.1.6. Is capable of tracking and managing risks in a virtual/cloud environment, if applicable.

Yes

4.1.7. Is capable of correlating incidents.

Yes

4.1.8. There is sufficient incident monitoring and detection coverage in accordance with government policies.

Yes

4.2. Please provide any additional information on the effectiveness of the Organization's Incident Management Program that was not noted in the questions above.

N/A

Section 5: RISK MANAGEMENT

5.1. Has the Organization established a risk management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines?

Yes

If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

5.1.1. Documented and centrally accessible policies and procedures for risk management, including descriptions of the roles and responsibilities of participants in this process.

Yes

5.1.2. Addresses risk from an organization perspective with the development of a comprehensive governance structure and organization-wide risk management strategy as described in NIST 800-37, Rev.1

Yes

Comments: SSA had a decentralized governance structure for IT security. This resulted in a system misconfiguration going undetected, enabling GT to obtain security and personally identifiable information. In addition, SSA lacked a centralized process to authorize hardware devices before they were connected to the Agency's network.

5.1.3. Addresses risk from a mission and business process perspective and is guided by the risk decisions at the organizational perspective, as described in NIST 800-37, Rev.1.

Yes

5.1.4. Addresses risk from an information system perspective and is guided by the risk decisions at the organizational perspective and the mission and business perspective, as described in NIST 800-37, Rev. 1.

Yes

5.1.5. Categorizes information systems in accordance with government policies.

Yes

5.1.6. Selects an appropriately tailored set of baseline security controls.

Yes

5.1.7. Implements the tailored set of baseline security controls and describes how the controls are employed within the information system and its environment of operation.

Yes

5.1.8. Assesses the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Yes

Comments: Financial statement audit testing found that SSA's vulnerability testing was insufficient.

5.1.9. Authorizes information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable.

Yes

5.1.10. Ensures information security controls are monitored on an ongoing basis including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.

Yes

Comments: SSA performed security authorizations and annual security testing of selected controls. However, SSA's continuous monitoring program was not fully implemented. See comment for Metric 1.2.

5.1.11. Information system specific risks (tactical), mission/business specific risks and organizational level (strategic) risks are communicated to appropriate levels of the organization.

Yes

5.1.12. Senior Officials are briefed on threat activity on a regular basis by appropriate personnel. (e.g., CISO).

Yes

5.1.13. Prescribes the active involvement of information system owners and common control providers, chief information officers, senior information security officers, authorizing officials, and other roles as applicable in the ongoing management of information system-related security risks.

Yes

5.1.14. Security authorization package contains system security plan, security assessment report, and POA&M in accordance with government policies.

Yes

5.1.15. Security authorization package contains Accreditation boundaries for Organization information systems defined in accordance with government policies.

Yes

5.2. Please provide any additional information on the effectiveness of the Organization's Risk Management Program that was not noted in the questions above.

Comments: Weaknesses identified in this area contributed to a financial statement audit material weakness identified by GT. Based on our work and evaluation of GT's work, we concluded that SSA had a FISMA significant deficiency.

Section 6: SECURITY TRAINING

6.1. Has the Organization established a security training program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines?

Yes

If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

6.1.1. Documented policies and procedures for security awareness training.

Yes

6.1.2. Documented policies and procedures for specialized training for users with significant information security responsibilities.

Yes

6.1.3. Security training content based on the organization and roles, as specified in Organization policy or standards.

Yes

6.1.4. Identification and tracking of the status of security awareness training for all personnel (including employees, contractors, and other Organization users) with access privileges that require security awareness training.

Yes

6.1.5. Identification and tracking of the status of specialized training for all personnel (including employees, contractors, and other Organization users) with significant information security responsibilities that require specialized training.

Yes

6.1.6. Training material for security awareness training contains appropriate content for the Organization.

Yes

6.2. Please provide any additional information on the effectiveness of the Organization's Security Training Program that was not noted in the questions above.

N/A

Section 7: PLAN OF ACTION & MILESTONES (POA&M)

7.1. Has the Organization established a POA&M program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and tracks and monitors known information security weaknesses?

Yes

If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

7.1.1. Documented policies and procedures for managing IT security weaknesses discovered during security control assessments and requiring remediation.

Yes

Comments: SSA's policy needed to be updated to reflect the current tools used to monitor and track security weaknesses.

7.1.2. Tracks, prioritizes and remediates weaknesses.

Yes

Comments: We found some IT security risks that were tracked, but not prioritized.

7.1.3. Ensures remediation plans are effective for correcting weaknesses.

Yes

7.1.4. Establishes and adheres to milestone remediation dates.

Yes

Comments: We noted several POA&Ms that did not include a scheduled completion date.

7.1.5. Ensures resources are provided for correcting weaknesses.

Yes

7.1.6. POA&Ms include security weaknesses discovered during assessments of security controls and requiring remediation. (Do not need to include security weakness due to a Risk Based Decision to not implement a security control).

Yes

7.1.7. Costs associated with remediating weaknesses are identified.

Yes

7.1.8. Program officials and contractors report progress on remediation to CIO on a regular basis, at least quarterly, and the CIO centrally

tracks, maintains, and independently reviews/validates the POA&M activities at least quarterly.

Yes

7.2. Please provide any additional information on the effectiveness of the Organization's POA&M Program that was not noted in the questions above.

N/A

Section 8: REMOTE ACCESS MANAGEMENT

8.1. Has the Organization established a remote access program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines?

Yes

If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

8.1.1. Documented policies and procedures for authorizing, monitoring, and controlling all methods of remote access.

Yes

8.1.2. Protects against unauthorized connections or subversion of authorized connections.

Yes

8.1.3. Users are uniquely identified and authenticated for all access.

Yes

8.1.4. Telecommuting policy is fully developed.

Yes

Comments: SSA's revised telework policy was in draft form, pending the resolution of administrative matters.

8.1.5. If applicable, multi-factor authentication is required for remote access.

Yes

8.1.6. Authentication mechanisms meet NIST Special Publication 800-63 guidance on remote electronic authentication, including strength mechanisms.

Yes

8.1.7. Defines and implements encryption requirements for information transmitted across public networks.

Yes

8.1.8. Remote access sessions, in accordance to OMB M-07-16, are timed-out after 30 minutes of inactivity after which re-authentication are required.

Yes

Comments: SSA exceeded best practice since its sessions time-out after 15 minutes of inactivity.

8.1.9. Lost or stolen devices are disabled and appropriately reported.

Yes

8.1.10. Remote access rules of behavior are adequate in accordance with government policies.

Yes

8.1.11. Remote access user agreements are adequate in accordance with government policies.

Yes

8.2. Please provide any additional information on the effectiveness of the Organization's Remote Access Management that was not noted in the questions above.

N/A

Section 9: CONTINGENCY PLANNING

9.1. Has the Organization established an enterprise-wide business continuity/disaster recovery program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines?

Yes

If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

9.1.1. Documented business continuity and disaster recovery policy providing the authority and guidance necessary to reduce the impact of a disruptive event or disaster.

Yes

9.1.2. The Organization has performed an overall Business Impact Analysis (BIA).

Yes

9.1.3. Development and documentation of division, component, and IT infrastructure recovery strategies, plans and procedures.

Yes

9.1.4. Testing of system specific contingency plans.

Yes

Comments: The Agency did not conduct contingency plan testing for 2 of the 21 major systems/applications. For one of the applications, the application owners were not aware of the annual testing requirement. For the other application, the application owners were working with the appropriate subject matter experts to integrate their application into SSA's disaster recovery exercise.

9.1.5. The documented business continuity and disaster recovery plans are in place and can be implemented when necessary.

Yes

9.1.6. Development and fully implementable of test, training, and exercise (TT&E) programs.

Yes

9.1.7. Performance of regular ongoing testing or exercising of business continuity/disaster recovery plans to determine effectiveness and to maintain current plans.

Yes

9.1.8. After-action report that addresses issues identified during contingency/disaster recovery exercises.

Yes

9.1.9. Systems that have alternate processing sites.

Yes

9.1.10. Alternate processing sites are subject to the same risks as primary sites.

Yes

9.1.11. Backups of information that are performed in a timely manner.

Yes

9.1.12. Contingency planning that consider supply chain threats.

Yes

Comments: SSA's two data centers will back up each other. SSA considered supply chain threats for one data center, but not the other.

9.2. Please provide any additional information on the effectiveness of the Organization's Contingency Planning Program that was not noted in the questions above.

N/A

Section 10: CONTRACTOR SYSTEMS

10.1. Has the Organization established a program to oversee systems operated on its behalf by contractors or other entities, including Organization systems and services residing in the cloud external to the Organization?

Yes

If yes, besides the improvement opportunities that may have been identified by the OIG, does the program includes the following attributes:

10.1.1. Documented policies and procedures for information security oversight of systems operated on the Organization's behalf by contractors or other entities, including Organization systems and services residing in public cloud.

Yes

10.1.2. The Organization obtains sufficient assurance that security controls of such systems and services are effectively implemented and comply with federal and Organization guidelines.

Yes

Comments: For 12 of 17 contractor systems identified by our testing, SSA either performed a security authorization or obtained documentation of the systems' compliance with Federal security guidelines. Three of the contractor systems were operated or owned by other Federal or State agencies. One was operated by a contractor whose services were used by many Federal agencies. SSA believed it was not responsible for performing a security authorization of this contractor system. The remaining contractor system was a Website, located in a public cloud, but did not have the proper security authorization. However, the Website contained non-sensitive, public information, and a link that redirected users to SSA's secure Website to report fraud allegations.

10.1.3. A complete inventory of systems operated on the Organization's behalf by contractors or other entities, including Organization systems and services residing in public cloud.

No

Comments: We found seven contractor systems that SSA had not identified on its inventory list.

10.1.4. The inventory identifies interfaces between these systems and Organization-operated systems.

Yes

10.1.5. The Organization requires appropriate agreements (e.g., MOUs, Interconnection Security Agreements, contracts, etc.) for interfaces between these systems and those that it owns and operates.

Yes

10.1.6. The inventory of contractor systems is updated at least annually.

Yes

10.1.7. Systems that are owned or operated by contractors or entities, including Organization systems and services residing in public cloud, are compliant with FISMA requirements, OMB policy, and applicable NIST guidelines.

Yes

Comments: See comments for Metric 10.1.2.

10.2. Please provide any additional information on the effectiveness of the Organization's Contractor Systems Program that was not noted in the questions above.

Comments: We found some IT-related contracts did not contain the proper FISMA security clause requirements.

Section 11: SECURITY CAPITAL PLANNING

11.1. Has the Organization established a security capital planning and investment program for information security?

Yes

If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

11.1.1. Documented policies and procedures to address information security in the capital planning and investment control (CPIC) process.

Yes

11.1.2. Includes information security requirements as part of the capital planning and investment process.

Yes

11.1.3. Establishes a discrete line item for information security in organizational programming and documentation.

Yes

11.1.4. Employs a business case/Exhibit 300/Exhibit 53 to record the information security resources required.

Yes

Comments: We identified inconsistencies in the supporting documents for some line items in Exhibit 53B. For example, some Exhibit 53B numbers were based on budget estimates rather than budget decisions.

11.1.5. Ensures that information security resources are available for expenditure as planned.

Yes

11.2. Please provide any additional information on the effectiveness of the Organization's Security Capital Planning Program that was not noted in the questions above.

N/A

Scope and Methodology

The *Federal Information Security Management Act of 2002* (FISMA) directs each agency's Inspector General to perform, or have an independent external auditor perform, an annual independent evaluation of the agency's information security programs and practices, as well as a review of an appropriate subset of agency systems. We contracted with Grant Thornton LLP (GT) to audit the Social Security Administration's (SSA) Fiscal Year (FY) 2012 financial statements. Because of the extensive internal control system work that is completed as part of that audit, our FISMA review requirements were incorporated into the GT financial statement audit contract. This evaluation included the *Federal Information System Controls Audit Manual* level reviews of SSA's financial-related information systems. GT also performed an "agreed-upon procedures" engagement using FISMA; Department of Homeland Security (DHS) Federal Information Security Memorandum 12-02, *FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*; National Institute of Standards and Technology guidance; the *Federal Information System Controls Audit Manual*; and other relevant security laws and regulations as a framework to complete the Inspector General-required review of SSA's information security program and practices and its information systems.

The results of our FISMA review are based on our evaluation of GT's FY 2012 financial statement audit and agreed-upon procedures work papers as well as various audits by our office. We also reviewed SSA's draft 2012 FISMA *Chief Information Officer Section Report*.

Our evaluation followed the DHS FY 2012 FISMA guidance[1] and focused on Risk Management, Configuration Management, Incident Response and Reporting, Security Training, Plan of Action and Milestones, Remote Access Management, Identity and Access Management, Continuous Monitoring Management, Contingency Planning, Contractor Systems, and Security Capital Planning.

We performed field work at SSA facilities nationwide from April to October 2012. We considered the results of our other audits performed in FY 2012. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[1] DHS Federal Information Security Memorandum 12-02, *FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, February 15, 2012.

The Social Security Administration's Major Systems

	System	Acronym
	General Support Systems[1]	
1	Audit Trail System	ATS
2	Comprehensive Integrity Review Process	CIRP
3	Death Alert Control and Update System	DACUS
4	Debt Management System	DMS
5	Enterprise Wide Mainframe & Distributed Network Telecommunications Services and System	EWANS
6	FALCON Data Entry System	FALCON
7	Human Resources Management Information System	HRMIS
8	Integrated Client Database System	ICDB
9	Integrated Disability Management System	IDMS
10	Quality System	QA
11	Security Management Access Control System	SMACS
12	Social Security Online Accounting & Reporting System	SSOARS
13	Social Security Unified Measurement System	SUMS
	Major Applications[2]	
1	Electronic Disability System	eDib

[1] Office of Management and Budget Circular A-130, Appendix III, *Security of Federal Automated Information Resources*, Section A.2.c, defines a "general support system" or "system" as an interconnected set of information resources under the same direct management control which shares common functionality.

[2] Office of Management and Budget Circular A-130, Appendix III, *Security of Federal Automated Information Resources*, Section A.2.d, defines a "major application" as an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.

	System	Acronym
2	Earnings Record Maintenance System	ERMS
3	National Investigative Case Management System	NICMS
4	Recovery of Overpayments, Accounting and Reporting System	ROAR
5	Retirement, Survivors, Disability Insurance Accounting System	RSDI ACCTNG
6	Supplemental Security Income Record Maintenance System	SSIRMS
7	Social Security Number Establishment and Correction System	SSNECS
8	Title II	T2

OIG Contacts and Staff Acknowledgments

OIG Contacts

Brian Karpe, Director, Information Technology Audit Division

Grace Chi, Audit Manager

Acknowledgments

In addition to those named above:

Michael Zimmerman, Auditor- in-Charge

Tina Nevels, Auditor-in-Charge

Asad Isfahani, Auditor

For additional copies of this report, please visit our Website at http://oig.ssa.gov/ or contact the Office of the Inspector General's Public Affairs Staff at (410) 965-4518. Refer to Common Identification Number A-14-12-12120.

Overview of the Office of the Inspector General

The Office of the Inspector General (OIG) is comprised of an Office of Audit (OA), Office of Investigations (OI), Office of the Counsel to the Inspector General (OCIG), Office of External Relations (OER), and Office of Technology and Resource Management (OTRM). To ensure compliance with policies and procedures, internal controls, and professional standards, the OIG also has a comprehensive Professional Responsibility and Quality Assurance program.

Office of Audit

OA conducts financial and performance audits of the Social Security Administration's (SSA) programs and operations and makes recommendations to ensure program objectives are achieved effectively and efficiently. Financial audits assess whether SSA's financial statements fairly present SSA's financial position, results of operations, and cash flow. Performance audits review the economy, efficiency, and effectiveness of SSA's programs and operations. OA also conducts short-term management reviews and program evaluations on issues of concern to SSA, Congress, and the general public.

Office of Investigations

OI conducts investigations related to fraud, waste, abuse, and mismanagement in SSA programs and operations. This includes wrongdoing by applicants, beneficiaries, contractors, third parties, or SSA employees performing their official duties. This office serves as liaison to the Department of Justice on all matters relating to the investigation of SSA programs and personnel. OI also conducts joint investigations with other Federal, State, and local law enforcement agencies.

Office of the Counsel to the Inspector General

OCIG provides independent legal advice and counsel to the IG on various matters, including statutes, regulations, legislation, and policy directives. OCIG also advises the IG on investigative procedures and techniques, as well as on legal implications and conclusions to be drawn from audit and investigative material. Also, OCIG administers the Civil Monetary Penalty program.

Office of External Relations

OER manages OIG's external and public affairs programs, and serves as the principal advisor on news releases and in providing information to the various news reporting services. OER develops OIG's media and public information policies, directs OIG's external and public affairs programs, and serves as the primary contact for those seeking information about OIG. OER prepares OIG publications, speeches, and presentations to internal and external organizations, and responds to Congressional correspondence.

Office of Technology and Resource Management

OTRM supports OIG by providing information management and systems security. OTRM also coordinates OIG's budget, procurement, telecommunications, facilities, and human resources. In addition, OTRM is the focal point for OIG's strategic planning function, and the development and monitoring of performance measures. In addition, OTRM receives and assigns for action allegations of criminal and administrative violations of Social Security laws, identifies fugitives receiving benefit payments from SSA, and provides technological assistance to investigations.